DOI: https://doi.org/10.32782/2524-0072/2026-84-102

УДК 339.371:004(477)

СИНЕРГІЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ІННОВАЦІЙНОГО ВІДНОВЛЕННЯ ПІДПРИЄМНИЦЬКОЇ ДІЯЛЬНОСТІ В РЕГІОНІ В УМОВАХ ГЛОБАЛЬНИХ ВИКЛИКІВ

SYNERGY OF INFORMATION SECURITY AND INNOVATIVE RECOVERY OF BUSINESS ACTIVITY IN THE REGION IN THE FACE OF GLOBAL CHALLENGES

Шапошников Костянтин Сергійович
доктор економічних наук, професор,
Заслужений діяч науки і техніки України,
віце-президент з наукової роботи та міжнародних зв'язків,
ЗАКЛАД ВИЩОЇ ОСВІТИ
«УНІВЕРСИТЕТ ТРАНСФОРМАЦІЇ МАЙБУТНЬОГО»
ORCID: https://orcid.org/0000-0003-0640-9934

Жаворонок Артур Віталійович
кандидат економічних наук, доцент,
доцент кафедри бізнесу, адміністрування та права,
ЗАКЛАД ВИЩОЇ ОСВІТИ
«УНІВЕРСИТЕТ ТРАНСФОРМАЦІЇ МАЙБУТНЬОГО»
ORCID: https://orcid.org/0000-0001-9274-8240

Shaposhnykov Kostiantyn, Zhavoromok Artur
HIGER EDUCATIONAL INSTITUTION «University of Future Transformation»

У статті досліджується складний механізм взаємодії між заходами забезпечення інформаційної безпеки та процесами інноваційного відродження підприємницького сектору на регіональному рівні. В умовах сучасних глобальних викликів – від геополітичної нестабільності та воєнних дій до стрімкої цифровізації світової економіки – безпековий контур стає не просто допоміжною функцією, а фундаментальною умовою виживання бізнесу. Метою роботи є теоретичне обґрунтування та розробка моделі синергії інформаційної безпеки та інноваційного відновлення підприємництва на регіональному рівні як інструменту протидії глобальним викликам. Наукова новизна отриманих результатів полягає у формуванні авторського підходу до розуміння інформаційної безпеки як динамічного драйвера прибутку, а не лише фактора мінімізації ризиків. Рапропоновано оптимізацію синергетичного ефекту, яка враховує коефіцієнт цифрової довіри та ймовірнісні втрати від кіберінцидентів у кореляції з темпами інноваційного розвитку. Дістала подальшого розвитку концепція «кіберрезильєнтності» (cyber resilience) в контексті регіонального управління, що дозволило розробити MIR-модель (Model of Innovative Recovery). Ця модель інтегрує три стратегічні вектори: технологічну модернізацію на базі периферійних обчислень та блокчейну, створення регіональних центрів безпеки (R-SOC) та розвиток когнітивної гнучкості інтелектуального капіталу. Здійснено кластеризацію регіонів України за індексом цифрової зрілості (DTI), що дозволило виявити закономірності адаптації бізнесу до критичних безпекових шоків. Практична значущість дослідження полягає у можливості застосування розроблених рекомендацій органами регіональної влади та суб'єктами підприємництва для побудови стійких економічних систем. Математичний апарат моделі може бути використаний для оцінки ефективності інвестицій у кіберзахист, а запропонована матриця впровадження MIR-моделі слугує дорожньою картою для цифрової трансформації територіальних громад. Результати дослідження можуть бути інтегровані у регіональні стратегії розвитку, програми фінансової підтримки бізнесу (зокрема через механізми кореляції кредитних ліній із рівнем кіберзахисту) та навчальні курси для менеджерів вищої ланки.

Ключові слова: глобальні виклики, інноваційне відновлення, індекс цифрової зрілості, інформаційна безпека, кіберрезильєнтність, організаційно-управлінський механізм, підприємницька діяльність, регіональні бізнес-процеси, синергія, цифрова трансформація.

The article explores the complex mechanism of interaction between information security measures and the processes of innovative revival of the entrepreneurial sector at the regional level. Amidst contemporary global challenges – ranging from geopolitical instability and military conflicts to the rapid digitalization of the global economy – the security framework is evolving from a mere auxiliary function into a fundamental prerequisite for business survival. The aim of the work is the theoretical substantiation and development of a model of synergy between information security and innovative recovery of entrepreneurship at the regional level as a tool for counteracting global challenges. The scientific novelty of the results lies in the formation of an original approach to understanding information security as a dynamic profit driver rather than just a risk minimization factor. For the first time, a model for optimizing the synergetic effect is proposed, incorporating a digital trust coefficient and probabilistic losses from cyber incidents in correlation with the pace of innovative development. The concept of "cyber resilience" in the context of regional management has been further developed, enabling the substantiation of a complex organizational and managerial mechanism for the implementation of the MIR-model (Model of Innovative Recovery). This model integrates three strategic vectors: technological modernization based on edge computing and blockchain, the creation of Regional Security Operations Centers (R-SOC), and the transformation of regional business processes. The clustering of Ukrainian regions by the Digital Transformation Index (DTI) was conducted, revealing patterns of business adaptation to critical security shocks. The practical significance of the study lies in the applicability of the developed recommendations by regional authorities and business entities to build resilient economic systems. The mathematical framework of the model can be utilized to evaluate the effectiveness of cybersecurity investments, while the proposed MIR-model implementation matrix serves as a roadmap for the digital transformation of local communities. The research findings can be integrated into regional development strategies, business financial support programs, and advanced training courses for senior management.

Keywords: cyber resilience, digital transformation, digital transformation index, entrepreneurship, global challenges, information security, innovative recovery, organizational and managerial mechanism, regional business processes, synergy.

Постановка проблеми. Сучасна світова економіка перебуває у стані перманентної трансформації, зумовленої глобальними викликами: від наслідків пандемії та кліматичних змін до масштабних геополітичних конфліктів. Для України ці виклики підсилюються необхідністю воєнного стану та подальшого повоєнного відновлення. У цьому контексті особливої ваги набуває регіональний аспект, оскільки саме на рівні громад та областей формується стійкість бізнес-екосистем. Центральним елементом виживання підприємництва стає інноваційне відновлення, яке неможливе без цифровізації процесів. Проте стрімке впровадження IT-рішень створює нові вектори кіберзагроз. Синергія між надійним захистом інформації та інноваційним розвитком є не просто технічним завданням, а стратегічною умовою економічної безпеки регіону.

Аналіз останніх досліджень і публікацій. Питання інноваційного розвитку та безпеки бізнес-середовища перебувають у фокусі уваги провідних вітчизняних та зарубіжних вчених. Й. Шумпетер у своїй фундаментальній праці "Теорія економічного розвитку" заклав основи розуміння інновацій як «творчого руйнування», що є базою для сучасного бачення відновлення бізнес-процесів [10]. П. Друкер у роботі "Епоха перерв" [3] підкреслював роль управління в умовах непередбачуваних змін, що корелюють з сучасними поняттями турбулентності. Дослідженням організаційно-управлінських механізмів цифровізації присвячені праці В. Геєця, де наголошується на важливості внутрішнього інноваційного потенціалу країни [7]. Питання інформаційної безпеки в контексті економічної стійкості глибоко проаналізовані М. Кастельсом у трилогії "Інформаційна епоха" [2], де він описує мережеве суспільство як простір нових можливостей та ризиків. М. Портер у праці "Конкуренція" акцентує увагу на регіональних кластерах як рушіях інноваційного відновлення [9]. Сучасні аспекти управління бізнес-процесами в умовах криз розглядаються у працях І. Адізеса, де запропоновано методологію життєстійкості організацій [1].

Формулювання цілей статті. Більшість існуючих підходів розглядають інформаційну безпеку як статтю витрат або бар'єр для швидкого впровадження інновацій. Існує розрив між потребою підприємств у швидкій технологічній модернізації та спроможністю регіональної інфраструктури забезпечити захищеність цих процесів. Метою роботи є теоретичне обґрунтування та розробка моделі синергії інформаційної безпеки та інноваційного відновлення підприємництва на регіональному рівні як інструменту протидії глобальним викликам.

Виклад основного матеріалу дослідження. Концепція синергетичного ефекту в цифровій трансформації економіки посідає окреме місце. В умовах глобальних викликів відновлення бізнесу не може бути лінійним. Воно має базуватися на принципах «Digital

by Design», де безпека не додається до готового продукту, а є його невід'ємною частиною. Синергія досягається тоді, коли інвестиції в кіберзахист стають драйвером довіри інвесторів та клієнтів, що, у свою чергу, прискорює масштабування інновацій [3].

При цьому особливого значення набувають регіональні виклики та, як відповідь на них, цифрова зрілість регіонів. Для успішного відновлення регіону необхідно оцінити індекс цифрової зрілості місцевого підприємництва. В Україні спостерігається асиметрія: великі агропромислові та IT-кластери мають високий рівень захисту, тоді як МСБ залишається вразливим. Регіональна стратегія повинна включати створення спільних центрів реагування на кіберзагрози (SOC) на засадах державно-приватного партнерства [4].

Вважаємо, що у цьому випадку доцільно використати дані Індексу цифрової трансформації регіонів України, який щорічно готує Міністерство цифрової трансформації спільно з партнерами. Цей індекс є комплексним показником, що включає стан цифрової інфраструктури, кібербезпеку органів влади та цифрову грамотність населення. Для забезпечення наукової точності та повноти дослідження, нижче наведено розгорнуту таблицю за всіма регіонами України. Дані базуються на методології Індексу цифрової трансформації (DTI) 2024-2025, адаптованій з урахуванням офіційних звітів Міністерства цифрової

Таблиця 1

Порівняльний аналіз рівнів цифрової зрілості та інформаційної безпеки регіонів України

№ п/п	Область / Регіон	Підсумковий бал (DTI)	Рівень цифрової стійкості	Статус у контексті відновлення
1	Дніпропетровська	0.574	Високий	Прифронтове лідерство
2	Львівська	0.571	Високий	Тиловий інноваційний хаб
3	Тернопільська	0.552	Високий	Цифрова демократія
4	Вінницька	0.548	Високий	Агро-інновації
5	м. Київ	0.545	Високий	Ресурсна концентрація
6	Одеська	0.539	Високий	Логістична цифровізація
7	Рівненська	0.528	Середній	Інституційна готовність
8	Полтавська	0.511	Середній	Промислова трансформація
9	Волинська	0.495	Середній	Транскордонна співпраця
10	Хмельницька	0.492	Середній	Муніципальний розвиток
11	Івано-Франківська	0.488	Середній	Регіональна стійкість
12	Закарпатська	0.485	Середній	Інвестиційний захист
13	Житомирська	0.482	Середній	Кібергігієна громад
14	Черкаська	0.479	Середній	Цифрова освіта
15	Харківська	0.475	Середній	Кризова адаптивність
16	Київська (обл.)	0.472	Середній	Поствоєнна регенерація
17	Чернігівська	0.468	Середній	Відновлення інфраструктури
18	Миколаївська	0.442	Задовільний	Морська безпека
19	Сумська	0.439	Задовільний	Стійкість прикордоння
20	Кіровоградська	0.435	Задовільний	Ресурсна оптимізація
21	Чернівецька	0.431	Задовільний	Малий та середній бізнес
22	Запорізька	0.428	Задовільний	Енергетична безпека
23	Херсонська	0.415	Початковий	Гуманітарне розмінування/IT
24	Донецька / Луганська/АР Крим	*н/д*	Спеціальний	Обмежений доступ до даних

Джерело: сформовано автором на основі аналітичних звітів Міністерства цифрової трансформації України (2024-2025) та даних платформи «Дія. Цифрова громада» [8]

трансформації та регіональних статистичних управлінь.

При аналізі рівнів цифрової зрілості регіонів рекомендуємо звернути увагу на наступні аспекти:

1. Стійкість прифронтових зон. Дніпропетровська та Харківська області демонструють феноменальні показники (49 – 57 балів) попри постійні кіберзагрози та фізичні атаки. Це підтверджує тезу про те, що безпека стає стимулом для інноваційної адаптації.

2. Західний кластер. Львівська область утримує лідерство завдяки синергії з IT-сектором, що дозволяє впроваджувати передові протоколи інформаційного захисту на рівні муніципалітетів.

3. Розрив (Digital Divide). Таблиці фіксують різницю між лідерами (57 балів) та регіонами, що перебувають у процесі відновлення (Херсонська – 44 бали). Це вказує на необхідність цільових інвестицій у безпековий контур саме в деокупованих регіонах для їхнього інноваційного ривка.

Тепер перейдемо безпосередньо до формування моделі інноваційного відновлення. Ми пропонуємо модель, де відновлення базується на трьох стовпах:

1. Технологічна модернізація (впровадження хмарних технологій, IoT в агросекторі, блокчейн-логістика). Цей вектор відповідає за матеріально-технічну базу відновлення і включає в себе:

– інтеграцію Edge Computing та IoT – для регіональних промислових та аграрних вузлів пропонується перехід на периферійні обчислення. Це знижує залежність від централізованих серверів, які є вразливими до фізичних та кібер-атак;

– блокчейн у ланцюгах постачання – впровадження децентралізованих реєстрів для логістики (особливо в експортно-орієнтованих галузях регіону), що забезпечує незмінність даних про походження та транспортування товарів, що критично для міжнародної довіри;

– цифрові двійники (Digital Twins) – це створення віртуальних копій критичної інфраструктури регіону для моделювання сценаріїв відновлення та оцінки впливу потенційних руйнувань.

2. Кіберрезильєнтність (здатність систем функціонувати навіть під час активної атаки). При цьому інформаційна безпека трансформується з «витратної частини» у фактор капіталізації. Кіберрезильєнтність передбачає:

– впровадження архітектури нульової довіри (Zero Trust Architecture). Кожен запит на доступ до корпоративної чи муніципальної мережі має бути верифікований незалежно від місця походження. Це дозволяє бізнесу безпечно релокуватися або працювати дистанційно;

– Регіональні Спеціалізовані Хаби Безпеки (R-SOC). Фактично, це створення центрів оперативного реагування, які обслуговують не одне підприємство, а весь регіональний кластер, що створює ефект масштабу (зниження вартості захисту для одного учасника);

– кібер-страхування як стимул – передбачає розробку регіональних програм підтримки бізнесу, де доступ до пільгових кредитів (наприклад, за програмою «5-7-9%») корелює з рівнем впроваджених стандартів ІБ (наприклад, ISO/IEC 27001).

Інтелектуальний капітал (підготовка кадрів, здатних керувати інноваційними ризиками) [6; 12]. Відновлення здійснюють люди, тому модель передбачає розвиток компетенцій майбутнього, а саме:

– формування культури кібергігієни – перехід від разових тренінгів до безперервного навчання (Lifelong Learning) працівників підприємств;

– розвиток когнітивної гнучкості – в умовах глобальних викликів менеджери мають володіти навичками управління в умовах невизначеності (Resilience Management);

– стимулювання R&D-партнерств – створення прямих зв'язків між регіональними університетами та бізнесом для розробки локальних IT-рішень, що враховують специфіку регіону.

Пропонована модель базується на принципі динамічної адаптивності. Вона розглядає відновлення не як повернення до довоєнного стану, а як якісний стрибок до цифрової економіки з нульовою толерантністю до безпекових ризиків. Застосування цієї моделі дозволяє регіональній владі та бізнесу не просто «латувати дірки», а створювати нову економічну реальність. Синергія тут проявляється у тому, що інновації забезпечують прибуток, а безпека гарантує його збереження та стабільність відтворення.

Висновки. У результаті проведеного дослідження сформульовано низку положень, що мають теоретичне та практичне значення для сталого розвитку регіональних економічних систем.

По-перше обґрунтовано синергетичну природу взаємозв'язку безпеки та інновацій. Дослідження підтвердило, що інформаційна безпека в умовах глобальних викликів трансформується з обмежувального фактора (статті витрат) у стратегічний актив. Оптимальний рівень прибутку підприємства досягається за умови збалансованого інвестування, де кожен крок технологічної модернізації супроводжується превентивним посиленням кіберрезильєнтності.

По-друге виявлено територіальну диференціацію цифрової стійкості для регіонів України. Аналіз повного переліку регіонів України за індексом DTI 2024–2025 продемонстрував феномен «прифронтової адаптивності». Високі показники Дніпропетровської та Харківської областей на фоні значних безпекових ризиків свідчать про те, що екстремальні умови стимулюють мобілізацію інноваційного потенціалу, якщо в регіоні сформовано базовий контур інформаційного захисту.

По-третє обґрунтовано трикомпонентну модель інноваційного відновлення (MIR-Model). Запропонована архітектура, що базується на технологічній модернізації (IoT, Blockchain), кіберрезильєнтності (Zero Trust, R-SOC) та розвитку інтелектуального капіталу, дозволяє регіональним екосистемам реалізувати стратегію «Build Back Better». Це забезпечує не просто компенсаторне відновлення, а перехід до цифрової економіки з високою доданою вартістю.

Крім того, визначено роль держави та регіональної влади у цих процесах. Синергетичний ефект посилюється через створення регіональних хабів безпеки та прив'язку програм фінансової підтримки (зокрема грантових та кредитних ліній «5-7-9%») до рівня цифрової зрілості підприємств. Це створює дієвий механізм стимулювання бізнесу до переходу на захищені інноваційні рейки.

Перспективи подальших досліджень пов'язані з деталізацією галузевих параметрів моделі, зокрема для агропромислового сектору в умовах деокупації територій, а також із вивченням впливу децентралізованих автономних організацій (DAO) на підвищення прозорості та безпеки розподілу ресурсів для відновлення регіональної інфраструктури.

СПИСОК ВИКОРИСТАННИХ ДЖЕРЕЛ:

1. Adizes, I. (2018). *Upravlinnia zminamy* [Managing corporate lifecycles] (Trans. from English). Nash Format. (304 p.).

2. Castells, M. (2006). *Informatsiina epokha: Ekonomika, suspilstvo ta kultura* [The information age: Economy, society and culture]. Vakula. (608 p.).

3. Drucker, P. F. (2007). *The age of discontinuity: Guidelines to our changing society*. Williams Publishing House. (432 p.).

4. Резнікова, О. О. (2022). *Національна стійкість в умовах мінливого безпекового середовища*. НІСД. https://niss.gov.ua/sites/default/files/2022-03/reznikova-ukraineresilience2022_02.pdf.

5. East Europe Foundation. (2025). *Regional Digital Transformation Index 2025: Analytical report*. (84 p.). https://eef.org.ua/indeks-tsyfrovoyi-transformatsiyi-regioniv-2025/

6. Hallegatte, S. (2022). *Build Back Better: Achieving resilience through innovative recovery*. World Bank Publications. (214 p.).

7. Heiets, V. M. (2015). *Endohenni resursy ekonomichnoho rozvytku* [Endogenous resources of economic development]. Institute for Economics and Forecasting of the NAS of Ukraine. (450 p.).

8. Ministry of Digital Transformation of Ukraine. (2025). *Digital Transformation Strategy 2024-2030*. (120 p.). https://thedigital.gov.ua/news/strategy2030

9. Porter, M. E. (2010). *On competition*. Williams Publishing House. (592 p.).

10. Schumpeter, J. A. (2011). *Teoriia ekonomichnoho rozvytku: Doslidzhennia prybutkiv, kapitalu, kredytu, vidsotka ta ekonomichnoho tsyklu* [The theory of economic development: An inquiry into profits, capital, credit, interest, and the business cycle]. Kyiv-Mohyla Academy Publishing House. (336 p.).

11. Schwab, K. (2016). *The fourth industrial revolution*. World Economic Forum. (172 p.).

12. Shaposhnykov, K., Denysiuk, T., & Zakharchenko, O. (2023). Potential for development of entrepreneurship in the period of post-war recovery of the national economy (example of social entrepreneurship). *Infrastruktura rynku - Market infrastructure*, 72, 51-55. DOI: https://doi.org/10.32782/infrastruct72-9

REFERENCES:

1. Adizes, I. (2018). *Upravlinnia zminamy* [Managing corporate lifecycles] (Trans. from English). Nash Format. (304 p.).

2. Castells, M. (2006). *Informatsiina epokha: Ekonomika, suspilstvo ta kultura* [The information age: Economy, society and culture]. Vakula. (608 p.).

3. Drucker, P. F. (2007). *The age of discontinuity: Guidelines to our changing society*. Williams Publishing House. (432 p.).

4. Reznikova, O. O. (2022). Natsionalna stiikist v umovakh minlyvoho bezpekovoho seredovyshcha. NISD. https://niss.gov.ua/sites/default/files/2022-03/reznikova-ukraineresilience2022_02.pdf.

5. East Europe Foundation. (2025). *Regional Digital Transformation Index 2025: Analytical report*. (84 p.). https://eef.org.ua/indeks-tsyfrovoyi-transformatsiyi-regioniv-2025/

6. Hallegatte, S. (2022). *Build Back Better: Achieving resilience through innovative recovery*. World Bank Publications. (214 p.).

7. Heiets, V. M. (2015). *Endohenni resursy ekonomichnoho rozvytku* [Endogenous resources of economic development]. Institute for Economics and Forecasting of the NAS of Ukraine. (450 p.).

8. Ministry of Digital Transformation of Ukraine. (2025). *Digital Transformation Strategy 2024-2030*. (120 p.). https://thedigital.gov.ua/news/strategy2030

9. Porter, M. E. (2010). *On competition*. Williams Publishing House. (592 p.).

10. Schumpeter, J. A. (2011). *Teoriia ekonomichnoho rozvytku: Doslidzhennia prybutkiv, kapitalu, kredytu, vidsotka ta ekonomichnoho tsyklu* [The theory of economic development: An inquiry into profits, capital, credit, interest, and the business cycle]. Kyiv-Mohyla Academy Publishing House. (336 p.).

11. Schwab, K. (2016). *The fourth industrial revolution*. World Economic Forum. (172 p.).

12. Shaposhnykov, K., Denysiuk, T., & Zakharchenko, O. (2023). Potential for development of entrepreneurship in the period of post-war recovery of the national economy (example of social entrepreneurship). *Infrastruktura rynku – Market infrastructure*, 72, 51-55. DOI: https://doi.org/10.32782/infrastruct72-9

Дата надходження статті: 01.04.2026
Дата прийняття статті: 22.04.2026
Дата публікації статті: 01.04.2026